ダイナミック アクセス ポリシー

この章では、ダイナミック アクセス ポリシーを設定する方法を説明します。

ダイナミック アクセス ポリシーについて

VPN ゲートウェイは動的な環境で動作します。個々の VPN 接続には、頻繁に変更されるイントラネット設定、組織内の各ユーザーが持つさまざまなロール、および設定とセキュリティ レベルが異なるリモート アクセス サイトからのログインなど、複数の変数が影響する可能性があります。VPN環境でのユーザー認可のタスクは、スタティックな設定のネットワークでの認可タスクよりもかなり複雑です。

ASA ではダイナミック アクセス ポリシー（DAP）によって、これらのさまざまな変数に対処する認可機能を設定できます。ダイナミック アクセス ポリシーは、特定のユーザー トンネルまたはユーザー セッションに関連付ける一連のアクセス コントロール属性を設定して作成します。これらの属性により、複数のグループ メンバーシップやエンドポイント セキュリティの問題に対処します。つまり、ASA では、定義したポリシーに基づき、特定のセッションへのアクセス権が特定のユーザーに付与されます。ASA は、ユーザーが接続した時点で、DAP レコードからの属性を選択または集約することによって DAP を生成します。DAP レコードは、リモート デバイスのエンドポイント セキュリティ情報および認証されたユーザーの AAA 認可情報に基づいて選択されます。選択された DAP レコードは、ユーザー トンネルまたはセッションに適用されます。

DAP システムには、注意を必要とする次のコンポーネントがあります。

- DAP 選択コンフィギュレーション ファイル：セッション確立中に DAP レコードを選択して適用するために ASA が使用する、基準が記述されたテキスト ファイル。ASA 上に保存されます。ASDM を使用して、このファイルを変更したり、XML データ形式で ASA にアップロードしたりできます。DAP選択設定ファイルには、ユーザーが設定するすべての属性が記載されています。これには、AAA 属性、エンドポイント属性、およびネットワーク ACL と Web タイプ ACL のフィルタ、ポート転送、URL のリストとして設定されたアクセス ポリシーなどがあります。
- DfltAccess ポリシー：常に DAP サマリー テーブルの最後のエントリで、プライオリティは必ず0。デフォルトアクセスポリシーのアクセスポリシー属性を設定できますが、AAA 属性またはエンドポイント属性は含まれておらず、これらの属性は設定できません。DfltAccessPolicy は削除できません。また、サマリー テーブルの最後のエントリになっている必要があります。

詳細については、『*Dynamic Access Deployment Guide*』（https://supportforums.cisco.com/docs/DOC-1369）を参照してください。

DAP によるリモート アクセス プロトコルおよびポスチャ評価ツールのサポート

ASA は、管理者が設定したポスチャ評価ツールを使用してエンドポイント セキュリティ属性を取得します。このポスチャ評価ツールには、 Secure Firewall ポスチャモジュール、独立した HostScan/Secure Firewall ポスチャパッケージ、および NAC が含まれます。

次の表に、DAP がサポートしている各リモート アクセス プロトコル、その方式で使用可能なポスチャ評価ツール、およびそのツールによって提供される情報を示します。

サポートされるリモート アクセス プロトコル	**Secure Firewall ポスチャモジュール** **ホスト スキャン パッケージ** **Secure Firewall ポスチャ**	**Secure Firewall ポスチャモジュール** **Hostscan パッケージ** **Secure Firewall ポスチャ**	**NAC**	**Cisco NAC アプライアンス**
	ファイル情報、レジストリ キーの値、実行プロセス、オペレーティング システムを返す	マルウェア対策およびパーソナル ファイアウォール ソフトウェアの情報を返す	NAC ステータスを返す	VLAN タイプと VLAN ID を返す
IPsec VPN	非対応	非対応	対応	対応

サポートされるリモート アクセス プロトコル	Secure Firewall ポスチャモジュール ホスト スキャン パッケージ Secure Firewall ポスチャ	Secure Firewall ポスチャモジュール Hostscan パッケージ Secure Firewall ポスチャ	NAC	Cisco NAC アプライアンス
Cisco AnyConnect VPN	対応	対応	対応	対応
クライアントレス（ブラウザベース）SSL VPN	対応	対応	非対応	非対応
PIX カットスループロキシ（ポスチャ評価は使用不可）	非対応	非対応	非対応	非対応

DAP によるリモート アクセス接続のシーケンス

次のシーケンスに、標準的なリモート アクセス接続を確立する場合の概要を示します。

1. リモート クライアントが VPN 接続を試みます。
2. ASA は、設定された NAC 値と HostScan/Secure Firewall ポスチャ値を使用してポスチャ評価を実行します。
3. ASA は、AAA を介してユーザーを認証します。AAA サーバーは、ユーザーの認可属性も返します。
4. ASA は AAA 認可属性をそのセッションに適用し、VPN トンネルを確立します。
5. ASA は、AAA 認可情報とセッションのポスチャ評価情報に基づいて DAP レコードを選択します。
6. ASA は選択した DAP レコードから DAP 属性を集約し、その集約された属性が DAP ポリシーになります。
7. ASA はその DAP ポリシーをセッションに適用します。

ダイナミック アクセス ポリシーのライセンス

（注） この機能は、ペイロード暗号化機能のないモデルでは使用できません。

ダイナミックアクセスポリシー（DAP）には、次のいずれかのライセンスが必要です。

- Secure Client Premier：すべての DAP 機能を使用する場合。
- Secure Client Advantage：オペレーティングシステムおよびオペレーティングシステムまたは セキュアクライアント のバージョンチェック専用。

関連トピック

DAP への セキュアクライアント エンドポイント属性の追加 （15 ページ）

ダイナミック アクセス ポリシーの設定

始める前に

- 特に記載のない限り、DAP エンドポイント属性を設定する前に、HostScan/Secure Firewall ポスチャをインストールする必要があります。
- HostScan 4.3.x から HostScan 4.6.x 以降にアップグレードする場合は、アップグレードの前に、既存の AV/AS/FW エンドポイント属性を対応する代替 AM/FW エンドポイント属性に移行する必要があります。アップグレードおよび移行の完全な手順については、『AnyConnect HostScan 4.3.x to 4.6.x Migration Guide』を参照してください。
- Java Web Start セキュリティの問題のため、デバイスで webvpn ベースの設定を使用する場合は、設定した値を高度なエンドポイント属性に入力できないことがあります。この問題を解決するには、ASDM デスクトップアプリケーションを使用するか、または Java セキュリティの例外として AEA 関連の URL を追加します。
- ファイル、プロセス、レジストリのエンドポイント属性を設定する前に、ファイル、プロセス、レジストリの基本HostScan/Secure Firewall ポスチャ属性を設定する必要があります。手順については、ASDM 内で適切な UI 画面に移動し、[ヘルプ（Help）] をクリックしてください。
- DAP は、ASCII 文字のみサポートされます。

手順

ステップ 1 ASDM を起動し、**[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [ダイナミックアクセスポリシー（Dynamic Access Policies）]** を選択します。

（注）
[Add]、[Edit]、および [Delete] アクションの下に [Incompatible] アクションボタンが表示される場合は、内部ライブラリの更新により既存 DAP ポリシー（HostScan 4.3.x 以前を使用して作成）と互換性がなくなったバージョン（4.6.x 以降）に HostScan をアップグレードしようとしています。ワンタイム移行手順を実行して、設定を適応させる必要があります。

[Incompatible] アクションが表示される場合は、HostScan のアップグレードが開始され、設定の移行が必要になったことを示しています。詳細な手順については、『AnyConnect Hostscan 4.3.x to 4.6.x Migration Guide』を参照してください。

ステップ 2 特定のマルウェア対策またはパーソナルファイアウォールのエンドポイント属性を含めるには、ペインの最上部近くの [設定（configuration）] リンクをクリックします。このリンクは、これら両方の機能をすでにイネーブルにしている場合には表示されません。

ステップ 3 設定済みの DAP のリストを表示します。

テーブルには次のフィールドが表示されます。

- [ACL Priority]：DAP レコードのプライオリティを表示します。

  ASA は、複数の DAP レコードからネットワーク ACL と Web タイプ ACL を集約するときに、この値を使用して ACL を論理的に順序付けします。ASA は、最上位のプライオリティ番号から最下位のプライオリティ番号の順にレコードを並べ、最下位のプライオリティをテーブルの一番下に配置します。番号が大きいほどプライオリティが高いことを意味します。たとえば、値が 4 の DAP レコードは値が 2 のレコードよりも高いプライオリティを持つことになります。プライオリティは、手動での並べ替えはできません。

- [Name]：DAP レコードの名前を表示します。
- [Network ACL List]：セッションに適用されるファイアウォール ACL の名前を表示します。
- [Web-Type ACL List]：セッションに適用される SSL VPN ACL の名前を表示します。
- [Description]：DAP レコードの目的を説明します。

ステップ 4 [Add] または [Edit] をクリックして、ダイナミック アクセス ポリシーの追加または編集 （6 ページ）を実行します。

ステップ 5 [Apply] をクリックして DAP 設定を保存します。

ステップ 6 [Find] フィールドを使用して、ダイナミック アクセス ポリシー（DAP）を検索します。

このフィールドへの入力を開始すると、DAP テーブルの各フィールドの先頭部分の文字が検索され、一致するものが検出されます。ワイルドカードを使用すると、検索範囲が広がります。

たとえば、[Find] フィールドに「**sal**」と入力した場合は、`Sales` という名前の DAP とは一致しますが、`Wholesalers` という名前の DAP とは一致しません。[Find] フィールドに ***sal** と入力すると、テーブル内の **Sales** または **Wholesalers** のうち、最初に出現したものが検出されます。

ステップ 7 ダイナミック アクセス ポリシーのテスト （8 ページ）を実行して設定を確認します。

ダイナミック アクセス ポリシーの追加または編集

手順

ステップ 1 ASDM を起動し、**[Configuration]** > **[Remote Access VPN]** > **[Network (Client) Access]** または **[Clientless SSL VPN Access]** > **[Dynamic Access Policies]** > **[Add]** または [Edit] を選択します。

ステップ 2 このダイナミック アクセス ポリシーの名前（必須）と説明（オプション）を入力します。

- [Policy Name] は、4 ～ 32 文字の文字列で、スペースは使用できません。
- DAP の [Description] フィールドには 80 文字まで入力できます。

ステップ 3 [ACL Priority] フィールドで、そのダイナミック アクセス ポリシーのプライオリティを設定します。

セキュリティ アプライアンスは、ここで設定した順序でアクセス ポリシーを適用します。数が大きいほどプライオリティは高くなります。有効値の範囲は 0 ～ 2147483647 です。デフォルト値は 0 です

ステップ 4 この DAP の選択基準を指定します。

a) [Selection Criteria] ペインのドロップダウン リスト（ラベルなし）で、ユーザーがこのダイナミック アクセス ポリシーを使用するには、すべてのエンドポイント属性を満たすことに加えて、ここで設定される AAA 属性値のいずれか（[ANY]）またはすべて（[ALL]）が必要となるのか、それとも一切不要（[NONE]）であるのかを選択します。

重複するエントリは許可されません。AAA 属性やエンドポイント属性を指定せずに DAP レコードを設定すると、レコードがすべての選択基準を満たしていることになるので、ASA は常にそのレコードを選択します。

b) [AAA Attributes] フィールドの [Add] または [Edit] をクリックして、DAP の AAA 属性選択基準の設定 （8 ページ）を実行します。

c) [Endpoint Attributes] 領域で [Add] または [Edit] をクリックして、DAP のエンドポイント属性選択基準の設定 （12 ページ）を実行します。

d) [Advanced] フィールドをクリックして、#unique_180を実行します。この機能を使用するには、Lua プログラミング言語の知識が必要です。

- [AND/OR]：基本的な選択ルールと、ここで入力する論理式との関係を定義します。つまり、すでに設定されている AAA 属性およびエンドポイント属性に新しい属性を追加するのか、またはそれら設定済みの属性に置き換えるのかを指定します。デフォルトは AND です。
- [Logical Expressions]：それぞれのタイプのエンドポイント属性のインスタンスを複数設定できます。新しい AAA 選択属性またはエンドポイント選択属性（あるいはその両方）を定義するフリー形式の LUA テキストを入力します。ASDM は、ここで入力されたテキストを検証せず、テキストを DAP XML ファイルにコピーするだけです。処理は ASA によって行われ、解析不能な式は破棄されます。

dap.xml ファイルのインポート/エクスポートについては、2 つの ASA 間で DAP XML ファイルをインポートおよびエクスポート （7 ページ）を参照してください。

ステップ 5 この DAP のアクセス/許可ポリシー属性を指定します。

ここで設定する属性値は、既存のユーザー、グループ、トンネル グループ、およびデフォルトのグループ レコードを含め、AAA システムの認可値を上書きします。DAP アクセスと許可ポリシー属性の設定 （34 ページ）を参照してください。

ステップ 6 [OK] をクリックします。

2 つの ASA 間で DAP XML ファイルをインポートおよびエクスポート

ASA のダイナミック アクセス ポリシー（DAP）設定は、ASA のフラッシュメモリ上の *dap.xml* というファイルに保存されます。このファイルには、DAP ポリシーの選択属性が含まれています。

（注） *dap.xml* ファイルをエクスポートして編集し（xml 構文を知っている場合）、再度インポートして戻すことはできますが、設定に誤りがあると、ASDM が DAP レコードの処理を停止する可能性があるため、十分に注意してください。構成のこの部分を操作する CLI はありません。

次の手順を使用して、2 つの ASA 間で *dap.xml* ファイルをインポートおよびエクスポートします。

手順では、ASA#1 から *dap.xml* ファイルをエクスポートし、ASA#2 にインポートする例を使用します。

ASDM を使用した ASA でのファイル処理については、『*Cisco ASA Series General Operations ASDM Configuration Guide*』の「*Managing Files*」の項を参照してください。

手順

ステップ 1 ASA#2 の *dap.xml* ファイルをクリアします。

a) ASA#2 の設定と *dap.xml* を外部の tftp または ftp サーバーに保存します。

b) ASA#2 の ASDM を終了します。

（注）
ASDM で ＞ [ツール（Tools）] > [バックアップの設定（BackUp Configurations）] > [DAP 設定（DAP Configurations）] オプションを使用して、*dap.xml* ファイルを保存することもできます。

ASA#2 フラッシュメモリ上の *dap.xml* ファイルの名前を変更または削除することもできます。

ステップ 2 ASA#2 コマンドプロンプトで、**clear configure dynamic-access-policy-record** コマンドを入力して、DAP レコードの構成を削除します。

ステップ 3 *dap.xml* ファイルを ASA#1 フラッシュからエクスポートし、ASA#2 フラッシュにインポートします。

ステップ 4 **dynamic-access-policy-record** コマンドを使用して、ASA#2 の ASA#1 からの DAP レコードエントリを設定します。

ステップ 5 ASA#2 で、**dynamic-access-policy-config activate** コマンドを使用して DAP を有効にします。

（注）
ASA#2 の ASDM を再起動して、DAP 設定をアクティブにすることもできます。

ステップ 6 ASA#2 で ASDM を再起動します。
新しい DAP ポリシーは ASA#2 で設定されます。

ダイナミック アクセス ポリシーのテスト

このペインでは、認可属性値のペアを指定することによって、デバイスで設定される DAP レコード セットが取得されるかどうかをテストできます。

手順

ステップ 1 属性値のペアを指定するには、[AAA Attribute] テーブルと [Endpoint Attribute] テーブルに関連付けられた [Add/Edit] ボタンを使用します。

[Add/Edit] ボタンをクリックすると表示されるダイアログは、[Add/Edit AAA Attributes] ウィンドウと [Add/Edit Endpoint Attributes] ダイアログボックスに表示されるダイアログに似ています。

ステップ 2 [Test] ボタンをクリックします。

デバイス上の DAP サブシステムは、各レコードの AAA およびエンドポイント選択属性を評価するときに、これらの値を参照します。結果は、[Test Results] 領域に表示されます。

DAP の AAA 属性選択基準の設定

DAP は AAA サービスを補完します。用意されている認可属性のセットは限られていますが、それらの属性によって AAA で提供される認可属性を無効にできます。AAA 属性は、Cisco AAA 属性階層から指定するか、ASA が RADIUS または LDAP サーバーから受信する応答属性一式から指定できます。ASA は、ユーザーの AAA 認可情報とセッションのポスチャ評価情報に基

づいて DAP レコードを選択します。ASA は、この情報に基づいて複数の DAP レコードを選択でき、それらのレコードを集約して DAP 認可属性を作成します。

手順

DAP レコードの選択基準として AAA 属性を設定するには、[Add/Edit AAA Attributes] ダイアログボックスで、使用する Cisco、LDAP、または RADIUS 属性を設定します。これらの属性は、入力する値に対して「=」または「!=」のいずれかに設定できます。各 DAP レコードに設定可能な AAA 属性の数に制限はありません。AAA 属性の詳細については、AAA 属性の定義 （11 ページ）を参照してください。

[AAA Attributes Type]：ドロップダウン リストを使用して、Cisco、LDAP、または RADIUS 属性を選択します。

- [Cisco]：AAA 階層モデルに保存されているユーザー認可属性を参照します。DAP レコードの AAA 選択属性に、これらのユーザー認可属性の小規模なサブセットを指定できます。次の属性が含まれます。
  - [Group Policy]：VPN ユーザー セッションに関連付けられているグループ ポリシー名を示します。セキュリティ アプライアンスでローカルに設定するか、IETF クラス（25）属性として RADIUS/LDAP から送信します。最大 64 文字です。
  - [Assigned IP Address]：ポリシーに指定する IPv4 アドレスを入力します。
  - [Assigned IPv6 Address]：ポリシーに指定する IPv6 アドレスを入力します。
  - [Connection Profile]：コネクションまたはトネリングのグループ名。最大 64 文字です。
  - [Username]：認証されたユーザーのユーザー名。最大 64 文字です。ローカル認証、RADIUS 認証、LDAP 認証のいずれかを、またはその他の認証タイプ（RSA/SDI、NT Domain などのいずれかを使用している場合に適用されます。
  - [=/!=]：と等しい/と等しくない
- [LDAP]：LDAP クライアントは、ユーザーの AAA セッションに関連付けられたデータベースにあるすべてのネイティブ LDAP 応答属性値のペアを保存します。LDAP クライアントでは、受信した順に応答属性をデータベースに書き込みます。その名前の後続の属性はすべて廃棄されます。ユーザー レコードとグループ レコードの両方が LDAP サーバーから読み込まれると、このシナリオが発生する場合があります。ユーザー レコード属性が最初に読み込まれ、グループ レコード属性よりも常に優先されます。

  Active Directory グループ メンバーシップをサポートするために、AAA LDAP クライアントでは、LDAP memberOf 応答属性に対する特別な処理が行われます。AD memberOf 属性は、AD 内のグループ レコードの DN 文字列を指定します。グループの名前は、DN 文字列内の最初の CN 値です。LDAP クライアントでは、DN 文字列からグループ名を抽出して、AAA memberOf 属性として格納し、応答属性データベースに LDAP memberOf 属性として格納します。LDAP 応答メッセージ内に追加の memberOf 属性が存在する場合、それらの属性からグループ名が抽出され、前の AAA memberOf 属性と結合されて、グループ名

がカンマで区切られた文字列が生成されます。この文字列は応答属性データベース内で更新されます。

LDAP 認証/認可サーバーへの VPN リモート アクセス セッションが次の 3 つの Active Directory グループ（memberOf 列挙）のいずれかを返す場合は、次の通りとなります。

cn=Engineering,ou=People,dc=company,dc=com

cn=Employees,ou=People,dc=company,dc=com

cn=EastCoastast,ou=People,dc=company,dc=com

ASA は、Engineering、Employees、EastCoast の 3 つの Active Directory グループを処理します。これらのグループは、aaa.ldap の選択基準としてどのような組み合わせでも使用できます。

LDAP 属性は、DAP レコード内の属性名と属性値のペアで構成されています。LDAP 属性名は、構文に従う必要があり、大文字、小文字を区別します。たとえば、AD サーバーが部門として返す値の代わりに、LDAP 属性の Department を指定した場合、DAP レコードはこの属性設定に基づき一致しません。

（注）
[Value] フィールドに複数の値を入力するには、セミコロン（;）をデリミタとして使用します。次に例を示します。

eng;sale; cn=Audgen VPN,ou=USERS,o=OAG

- [RADIUS]：RADIUS クライアントは、ユーザーの AAA セッションに関連付けられたデータベースにあるすべてのネイティブ RADIUS 応答属性値のペアを保存します。RADIUS クライアントは、受け取った順序で応答属性をデータベースに書き込みます。その名前の後続の属性はすべて廃棄されます。ユーザー レコードおよびグループ レコードの両方が RADIUS サーバーから読み込まれた場合、このシナリオが発生する可能性があります。ユーザー レコード属性が最初に読み込まれ、グループ レコード属性よりも常に優先されます。

  RADIUS 属性は、DAP レコード内の属性番号と属性値のペアで構成されています。

  （注）
  RADIUS 属性について、DAP は Attribute ID = 4096 + RADIUS ID と定義します。

  次に例を示します。

  RADIUS 属性「Access Hours」の Radius ID は 1 であり、したがって DAP 属性値は 4096 + 1 = 4097 となります。

  RADIUS 属性「Member Of」の Radius ID は 146 であり、したがって DAP 属性値は 4096 + 146 = 4242 となります。

- LDAP および RADIUS 属性には、次の値があります。
  - [Attribute ID]：属性の名前/番号。最大 64 文字です。
  - [Value]：属性名（LDAP）または数値（RADIUS）。

[Value] フィールドに複数の値を入力するには、セミコロン（;）をデリミタとして使用します。例：`eng;sale; cn=Audgen VPN,ou=USERS,o=OAG`

- [=/!=]：と等しい/と等しくない

- LDAP には、[Get AD Groups] ボタンが含まれます。Active Directory グループの取得 （11 ページ）を参照してください。

Active Directory グループの取得

Active Directory サーバーにクエリーを実行し、このペインで利用可能な AD グループを問い合わせることができます。この機能は、LDAP を使用している Active Directory サーバーだけに適用されます。このボタンは、Active Directory LDAP サーバーに対して、ユーザーが属するグループのリスト（memberOf 列挙）の問い合わせを実行します。このグループ情報を使用し、ダイナミック アクセス ポリシーの AAA 選択基準を指定します。

AD グループは、バックグランドで CLI の **how-ad-groups** コマンドを使用することで LDAP サーバーから取得されます。ASA がサーバーの応答を待つデフォルト時間は 10 秒です。aaa-server ホスト コンフィギュレーション モードで **group-search-timeout** コマンドを使用し、時間を調整できます。

[Edit AAA Server] ペインで Group Base DN を変更し、Active Directory 階層の中で検索を開始するレベルを変更できます。このウィンドウでは、ASA がサーバーの応答を待つ時間も変更できます。これらの機能を設定するには、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [AAA Server Groups] > [Edit AAA Server] を選択します。

（注） Active Directory サーバーに多数のグループが存在する場合は、サーバーが応答パケットに含めることのできるデータ量の制限に従って、取得した AD グループのリスト（または **show ad-groups** コマンドの出力）が切り詰められることがあります。この問題を回避するには、フィルタ 機能を使用し、サーバーが返すグループ数を減らしてください。

[AD Server Group]：AD グループを取得する AAA サーバー グループの名前。

[Filter By]：表示されるグループ数を減らすために、グループ名またはグループ名の一部を指定します。

[Group Name]：サーバーから取得された AD グループのリスト。

AAA 属性の定義

次の表に、DAP で使用できる AAA 選択属性名の定義を示します。属性名フィールドは、LUA 論理式での各属性名の入力方法を示しており、[Add/Edit Dynamic Access Policy] ペインの [Advanced] セクションで使用します。

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
シスコ	aaa.cisco.grouppolicy	AAA	string	64	ASA 上のグループ ポリシー名、または RADIUS/LDAP サーバーから IETF-CLass (25) 属性として送信されたグループ ポリシー名
	aaa.cisco.ipaddress	AAA	number	-	フルトンネル VPN クライアントに割り当てられた IP アドレス（IPsec、L2TP/IPsec、SSL VPN Anyconnect モジュール）
	aaa.cisco.tunnelgroup	AAA	string	64	接続プロファイル（トンネルグループ）の名前
	aaa.cisco.username	AAA	string	64	認証されたユーザーの名前（ローカル認証や認可を使用している場合に適用）
LDAP	aaa.ldap.<*label*>	LDAP	string	128	LDAP 属性値ペア
RADIUS	aaa.radius.<number>	RADIUS	string	128	RADIUS 属性値ペア

DAP のエンドポイント属性選択基準の設定

エンドポイント属性には、エンドポイント システム環境、ポスチャ評価結果、およびアプリケーションに関する情報が含まれています。ASA は、セッション確立時にエンドポイント属性の集合を動的に生成し、セッションに関連付けられているデータベースにそれらの属性を保存します。各 DAP レコードには、ASA がセッションの DAP レコードを選択するために満たす必要があるエンドポイント選択属性が指定されています。ASA は、設定されている条件をすべて満たす DAP レコードだけを選択します。

始める前に

- DAP レコードの選択基準としてエンドポイント属性を設定することは、ダイナミック アクセス ポリシーの設定 （4 ページ）のための大きなプロセスの一部です。DAP の選択基準としてエンドポイント属性を設定する前に、この手順を確認します。
- エンドポイント属性の詳細については、「エンドポイント属性の定義 （23 ページ）」を参照してください。
-

- メモリ常駐型のマルウェア対策、およびパーソナル ファイアウォール プログラムを HostScan/Secure Firewall ポスチャがチェックする方法の詳細については、DAP とマルウェア対策およびパーソナル ファイアウォール プログラム （22 ページ）を参照してください。

手順

ステップ 1 [Add] または [Edit] をクリックして、次のいずれかのエンドポイント属性を選択基準として追加します。

各タイプのエンドポイント属性のインスタンスを複数作成できます。各 DAP レコードに設定可能なエンドポイント属性の数に制限はありません。

- DAP へのマルウェア対策エンドポイント属性の追加 （14 ページ）
- DAP へのアプリケーション属性の追加 （14 ページ）
- DAP への セキュアクライアント エンドポイント属性の追加 （15 ページ）
- DAP へのファイル エンドポイント属性の追加 （17 ページ）
- DAP へのデバイス エンドポイント属性の追加 （17 ページ）
- DAP への NAC エンドポイント属性の追加 （18 ページ）
- DAP へのオペレーティング システム エンドポイント属性の追加 （19 ページ）
- DAP へのパーソナル ファイアウォール エンドポイント属性の追加 （19 ページ）
- DAP へのポリシー エンドポイント属性の追加 （20 ページ）
- DAP へのプロセス エンドポイント属性の追加 （20 ページ）
- DAP へのレジストリ エンドポイント属性の追加 （21 ページ）
- DAP への複数証明書認証属性の追加 （21 ページ）

ステップ 2 条件に一致する DAP ポリシーを指定します。

これらのエンドポイント属性のタイプごとに、ユーザーがあるタイプのインスタンスのすべてを持つように DAP ポリシーで要求する（Match all = AND、デフォルト）のか、またはそれらのインスタンスを 1 つだけ持つように要求する（Match Any = OR）のかを決定します。

a) [Logical Op] をクリックします。
b) エンドポイント属性のタイプごとに、[Match Any]（デフォルト）または [Match All] を選択します。
c) [OK] をクリックします。

ステップ 3 ダイナミック アクセス ポリシーの追加または編集 （6 ページ）に戻ってください。

DAP へのマルウェア対策エンドポイント属性の追加

始める前に

HostScan 4.3.x から HostScan 4.6.x 以降にアップグレードする場合は、アップグレードの前に、既存の AV/AS/FW エンドポイント属性を対応する代替 AM/FW エンドポイント属性に移行する必要があります。アップグレードおよび移行の完全な手順については、『AnyConnect HostScan 4.3.x to 4.6.x Migration Guide』を参照してください。

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Anti-Malware] を選択します。

ステップ 2 適切なボタン [Installed] または [Not Installed] をクリックして、選択したエンドポイント属性とそれに付随する修飾子（[Name]/[Operation]/[Value] 列の下のフィールド）をインストールするか、またはインストールしないかを指定します。

ステップ 3 リアルタイム スキャンを有効または無効のどちらにするかを決定します。

ステップ 4 [Vendor] リスト ボックスで、テスト対象のマルウェア対策ベンダーの名前をクリックします。

ステップ 5 [Product Description] チェックボックスをオンにして、テストするベンダーの製品名をリスト ボックスから選択します。

ステップ 6 [Version] チェックボックスをオンにして、操作フィールドを、[Version] リスト ボックスで選択した製品バージョン番号に等しい（=）、等しくない（!=）、より小さい（<）、より大きい（>）、以下（<=）、または以上（>=）に設定します。

リスト ボックスで選択したバージョンに x が付いている場合（たとえば 3.x）は、この x を具体的なリリース番号で置き換えます（たとえば 3.5）。

ステップ 7 [Last Update] チェックボックスをオンにします。最後の更新からの日数を指定します。更新を、ここで入力した日数よりも早く（[<]）実行するか、遅く（[>]）実行するかを指定できます。

ステップ 8 [OK] をクリックします。

DAP へのアプリケーション属性の追加

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Application] を選択します。

ステップ 2 [Client Type] の操作フィールドで、[=]（等しい）または [!=]（等しくない）を選択します。

ステップ 3 [Client type] リスト ボックスで、テスト対象のリモート アクセス接続のタイプを指定します。

ステップ 4 [OK] をクリックします。

DAP への セキュアクライアント エンドポイント属性の追加

セキュアクライアント エンドポイント属性（モバイルポスチャまたは AnyConnect アイデンティティ拡張機能（ACIDex）とも呼ばれる）は、Cisco Secure Clientの AnyConnect VPN モジュールが ASA にポスチャ情報を伝えるために使用されます。ダイナミック アクセス ポリシーでは、ユーザーの認証にこれらのエンドポイント属性が使用されます。

モバイルポスチャ属性をダイナミック アクセス ポリシーに組み込むと、エンドポイントに HostScan/Secure Firewall ポスチャがエンドポイントにインストールされていなくても適用できます。

一部のモバイルポスチャ属性は、モバイルデバイス上で実行しているセキュアクライアントにのみ関連します。その他のモバイルポスチャ属性は、モバイルデバイス上で実行している セキュアクライアントと セキュアクライアント デスクトップクライアント上で実行している AnyConnect クライアントの両方に関連します。

始める前に

モバイルポスチャを活用するには、セキュアクライアント Mobile ライセンスと、セキュアクライアント Premium ライセンスが ASA にインストールされている必要があります。これらのライセンスをインストールする企業は、DAP 属性および他の既存のエンドポイント属性に基づいてサポートされているモバイル デバイスの DAP ポリシーを適用できます。これには、モバイル デバイスからのリモート アクセスの許可または拒否が含まれます。

手順

ステップ 1 [エンドポイント属性タイプ（Endpoint Attribute Type）] リストボックスで セキュアクライアント を選択します。

ステップ 2 [クライアントバージョン（Client Version）] チェックボックスをオンにして、等しい（=）、等しくない（!=）、より小さい（<）、より大きい（>）、以下（<=）、または以上（>=）を操作フィールドで選択してから、[クライアントバージョン（Client Version）] フィールドで セキュアクライアントバージョン番号を指定します。

このフィールドを使用すると、モバイルデバイス（携帯電話やタブレットなど）のクライアント バージョンを評価できるほか、デスクトップやラップトップ デバイスのクライアント バージョンも評価できます。

ステップ 3 [Platform] チェックボックスをオンにして、等しい（=）または等しくない（!=）を操作フィールドで選択してから、[Platform] リスト ボックスでオペレーティング システムを選択します。

このフィールドを使用すると、モバイル デバイス（携帯電話やタブレットなど）のオペレーティング システムを評価できるほか、デスクトップやラップトップ デバイスのオペレーティ

ングシステムも評価できます。プラットフォームを選択すると、追加の属性フィールドである [Device Type] と [Device Unique ID] が使用可能になります。

ステップ 4 [Platform Version] チェックボックスをオンにして、等しい（=）、等しくない（!=）、より小さい（<）、より大きい（>）、以下（<=）、または以上（>=）を操作フィールドで選択してから、[Platform Version] フィールドでオペレーティング システム バージョン番号を指定します。

作成する DAP レコードにこの属性も含まれるようにするには、前の手順でプラットフォームも必ず指定してください。

ステップ 5 [Platform] チェックボックスをオンにした場合は、[Device Type] チェックボックスをオンにすることができます。等しい（=）または等しくない（!=）を操作フィールドで選択してから、デバイスを [Device Type] フィールドで選択するか入力します。

サポートされるデバイスであるにもかかわらず、[Device Type] フィールドのリストに表示されていない場合は、[Device Type] フィールドに入力できます。デバイスタイプ情報を入手する最も確実な方法は、セキュアクライアントをエンドポイントにインストールして ASA に接続し、DAP トレースを実行することです。DAP トレースの結果の中で、**endpoint.anyconnect.devicetype** の値を見つけます。この値を [Device Type] フィールドに入力する必要があります。

ステップ 6 [Platform] チェックボックスをオンにした場合は、[Device Unique ID] チェックボックスをオンにすることができます。等しい（=）または等しくない（!=）を操作フィールドで選択してから、デバイスの一意の ID を [Device Unique ID] フィールドに入力します。

[Device Unique ID] によって個々のデバイスが区別されるので、特定のモバイル デバイスに対するポリシーを設定できます。デバイスの一意の ID を取得するには、そのデバイスを ASA に接続して DAP トレースを実行し、**endpoint.anyconnect.deviceuniqueid** の値を見つける必要があります。この値を [Device Unique ID] フィールドに入力する必要があります。

ステップ 7 [Platform] をオンにした場合は、[MAC Addresses Pool] フィールドに MAC アドレスを追加できます。等しい（=）または等しくない（!=）を操作フィールドで選択してから、MAC アドレスを指定します。各 MAC アドレスのフォーマットは xx-xx-xx-xx-xx-xx であることが必要です。x は有効な 16 進数文字（0 ～ 9、A ～ F、または a ～ f）です。MAC アドレスは、1 つ以上の空白スペースで区切る必要があります。

MAC アドレスによって個々のシステムが区別されるので、特定のデバイスに対するポリシーを設定できます。システムの MAC アドレスを取得するには、そのデバイスを ASA に接続して DAP トレースを実行し、**endpoint.anyconnect.macaddress** の値を見つける必要があります。この値を [MAC Address Pool] フィールドに入力する必要があります。

ステップ 8 [OK] をクリックします。

DAP へのファイル エンドポイント属性の追加

始める前に

ファイルエンドポイント属性を設定する前に、どのファイルをスキャンするかを[HostScan/Secure Firewall ポスチャ（HostScan/Secure Firewall Posture）] ウィンドウで定義します。

HostScan バージョン 4.x の場合、ASDM で [設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [Secure Desktop Manager] > [HostScan] を選択します。Secure Firewall ポスチャバージョン 5.x の場合、ASDM で [設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ポスチャ（Secure Firewall用）（Posture (for Secure Firewall)）] > [ポスチャ設定（Posture Settings）] を選択します。

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [File] を選択します。

ステップ 2 [Exists] と [Does not exist] のオプション ボタンでは、選択したエンドポイント属性とそれに付随する修飾子（[Exists]/[Does not exist] ボタンの下にあるフィールド）が存在する必要があるかどうかに応じて、該当するものを選択します。

ステップ 3 [Endpoint ID] リスト ボックスで、スキャン対象のファイル エントリに等しいエンドポイント ID をドロップダウン リストから選択します。

ファイルの情報が [Endpoint ID] リスト ボックスの下に表示されます。

ステップ 4 [Last Update] チェックボックスをオンにしてから、更新日からの日数が指定の値よりも小さい（<）と大きい（>）のどちらを条件とするかを操作フィールドで選択します。更新日からの日数を [days] フィールドに入力します。

ステップ 5 [Checksum] チェックボックスをオンにしてから、テスト対象ファイルのチェックサム値と等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。

ステップ 6 [Compute CRC32 Checksum**]** をクリックすると、テスト対象のファイルのチェックサム値が計算されます。

ステップ 7 [OK] をクリックします。

DAP へのデバイス エンドポイント属性の追加

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Device] を選択します。

ステップ 2 [Host Name] チェックボックスをオンにしてから、テスト対象デバイスのホスト名と等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。完全修飾ドメイン名（FQDN）ではなく、コンピュータのホスト名のみを使用します。

ステップ 3 [MAC address] チェックボックスをオンにしてから、テスト対象のネットワーク インターフェイス カードの MAC アドレスと等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。1 つのエントリにつき MAC アドレスは 1 つだけです。アドレスのフォーマットは xxxx.xxxx.xxxx であることが必要です。x は 16 進数文字です。

ステップ 4 [BIOS Serial Number] チェックボックスをオンにしてから、テスト対象のデバイスの BIOS シリアル番号と等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。数値フォーマットは、製造業者固有です。フォーマット要件はありません。

ステップ 5 [TCP/UDP Port Number] チェックボックスをオンにしてから、テスト対象のリスニング状態の TCP ポートと等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。

TCP/UDP コンボ ボックスでは、テスト対象（TCP（IPv4）、UDP（IPv4）、TCP（IPv6）、または UDP（IPv6））のポートの種類を選択します。複数のポートをテストする場合は、DAP の個々のエンドポイント属性のルールをいくつか作成し、それぞれに 1 個のポートを指定します。

ステップ 6 [Version of Secure Desktop (CSD)] チェックボックスをオンにしてから、エンドポイント上で実行される HostScan/Secure Firewall ポスチャ イメージのバージョンと等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。

ステップ 7 [Version of Endpoint Assessment] チェックボックスをオンにしてから、テスト対象のエンドポイント アセスメント（OPSWAT）のバージョンと等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。

ステップ 8 [OK] をクリックします。

DAP への NAC エンドポイント属性の追加

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [NAC] を選択します。

ステップ 2 [Posture Status] チェックボックスをオンにしてから、ACS によって受信されるポスチャ トークン文字列と等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。ポスチャ トークン文字列を [Posture Status] テキスト ボックスに入力します。

ステップ 3 [OK] をクリックします。

DAP へのオペレーティング システム エンドポイント属性の追加

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Operating System] を選択します。

ステップ 2 [OS Version] チェックボックスをオンにしてから、[OS Version] リスト ボックスで設定するオペレーティング システム（Windows、Mac、または Linux）と等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。

ステップ 3 [OS Update] チェックボックスをオンにしてから、[OS Update] テキスト ボックスに入力する Windows、Mac、または Linux オペレーティング システムのサービス パックと等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。

ステップ 4 [OK] をクリックします。

DAP へのパーソナル ファイアウォール エンドポイント属性の追加

始める前に

HostScan 4.3.x から HostScan 4.6.x 以降にアップグレードする場合は、アップグレードの前に、既存の AV/AS/FW エンドポイント属性を対応する代替 AM/FW エンドポイント属性に移行する必要があります。アップグレードおよび移行の完全な手順については、『AnyConnect HostScan 4.3.x to 4.6.x Migration Guide』を参照してください。

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Operating System] を選択します。

ステップ 2 適切なボタン [Installed] または [Not Installed] をクリックして、選択したエンドポイント属性とそれに付随する修飾子（[Name]/[Operation]/[Valud] 列の下のフィールド）をインストールするか、またはインストールしないかを指定します。

ステップ 3 [Vendor] リスト ボックスで、テスト対象のパーソナル ファイアウォール ベンダーの名前をクリックします。

ステップ 4 [Product Description] チェックボックスをオンにして、テストするベンダーの製品名をリスト ボックスから選択します。

ステップ 5 [Version] チェックボックスをオンにして、操作フィールドを、[Version] リスト ボックスで選択した製品バージョン番号に等しい（=）、等しくない（!=）、より小さい（<）、より大きい（>）、以下（<=）、または以上（>=）に設定します。

[Version] リスト ボックスで選択したバージョンに x が付いている場合（たとえば 3.x）は、この x を具体的なリリース番号で置き換えます（たとえば 3.5）。

ステップ 6 [Last Update] チェックボックスをオンにします。最後の更新からの日数を指定します。更新を、ここで入力した日数よりも早く（[<]）実行するか、遅く（[>]）実行するかを指定できます。

ステップ 7 **[OK]** をクリックします。

DAP へのポリシー エンドポイント属性の追加

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Policy] を選択します。

ステップ 2 [Location] チェックボックスをオンにしてから、Cisco Secure Desktop Microsoft Windows ロケーション プロファイルと等しい（=）または等しくない（!=）のどちらを条件とするかを操作フィールドで選択します。Cisco Secure Desktop Microsoft Windows ロケーション プロファイル文字列を [Location] テキスト ボックスに入力します。

ステップ 3 [OK] をクリックします。

DAP へのプロセス エンドポイント属性の追加

始める前に

プロセスエンドポイント属性を設定する前に、どのプロセスをスキャンするかを Cisco Secure Desktop の [HostScan/Secure Firewallポスチャ（HostScan/Secure Firewall Posture）] ウィンドウで定義します。

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Process] を選択します。

ステップ 2 [Exists] または [Does not exist] のボタンでは、選択したエンドポイント属性とそれに付随する修飾子（[Exists]/[Does not exist] ボタンの下にあるフィールド）が存在する必要があるかどうかに応じて、該当するものをクリックします。

ステップ 3 [Endpoint ID] リスト ボックスで、スキャン対象のエンドポイント ID をドロップダウン リストから選択します。

エンドポイント ID プロセス情報がリスト ボックスの下に表示されます。

ステップ 4 [OK] をクリックします。

DAP へのレジストリ エンドポイント属性の追加

レジストリ エンドポイント属性のスキャンは Windows オペレーティング システムにのみ適用されます。

始める前に

レジストリエンドポイント属性を設定する前に、どのレジストリキーをスキャンするかを [HostScan/Secure Firewall ポスチャ（HostScan/Secure Firewall Posture）] ウィンドウで定義します。

手順

ステップ 1 [Endpoint Attribute Type] リスト ボックスで [Registry] を選択します。

ステップ 2 [Exists] または [Does not exist] のボタンでは、レジストリ エンドポイント属性とそれに付随する修飾子（[Exists]/[Does not exist] ボタンの下にあるフィールド）が存在する必要があるかどうかに応じて、該当するものをクリックします。

ステップ 3 [Endpoint ID] リスト ボックスで、スキャン対象のレジストリ エントリに等しいエンドポイント ID をドロップダウン リストから選択します。

レジストリの情報が [Endpoint ID] リスト ボックスの下に表示されます。

ステップ 4 [Value] チェックボックスをオンにしてから、操作フィールドで等しい（=）または等しくない（!=）を選択します。

ステップ 5 最初の [Value] リスト ボックスで、レジストリ キーが dword か文字列かを指定します。

ステップ 6 2 つ目の [Value] 操作リスト ボックスに、スキャン対象のレジストリ キーの値を入力します。

ステップ 7 スキャン時にレジストリ エントリの大文字と小文字の違いを無視するには、チェックボックスをオンにします。検索時に大文字と小文字を区別するには、チェックボックスをオフにしてください。

ステップ 8 [OK] をクリックします。

DAP への複数証明書認証属性の追加

受信した証明書のいずれかを設定されたルールで参照できるように各証明書をインデックス化できます。これらの証明書フィールドに基づいて、接続試行を許可または拒否する DAP ルールを設定できます。

手順

ステップ 1 **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Dynamic Access Policies] > [Add Endpoint Attribute]** の順に移動します。

ステップ 2 [Endpoint Attribute Type] としてドロップダウン メニューの [Multiple Certificate Authentication] を選択します。

ステップ 3 必要に応じて次のいずれかまたはすべてを設定します。

- Subject Name
- 発行元名
- Subject Alternate Name
- Serial Number

ステップ 4 証明書ストアをデフォルトの [None] のままにしていずれのストアからの証明書も許可するか、ユーザーのみまたはマシンのみを許可するように選択します。[User] または [Machine] を選択する場合、証明書の元のストアを入力する必要があります。この情報は、プロトコルでクライアントによって送信されます。

DAP とマルウェア対策およびパーソナル ファイアウォール プログラム

セキュリティ アプライアンスは、ユーザー属性が、設定済みの AAA 属性およびエンドポイント属性に一致する場合に DAP ポリシーを使用します。プリログイン評価モジュールおよび HostScan/Secure Firewall ポスチャは、設定済みエンドポイント属性の情報をセキュリティアプライアンスに返し、DAP サブシステムでは、その情報に基づいてそれらの属性値に一致する DAP レコードを選択します。

マルウェア対策およびパーソナルファイアウォールプログラムのほとんど（すべてではなく）は、アクティブ スキャンをサポートしています。つまり、それらのプログラムはメモリ常駐型であり、常に動作しています。HostScan/Secure Firewall ポスチャは、エンドポイントにプログラムがインストールされているかどうか、およびそのプログラムがメモリ常駐型かどうかを、次のようにしてチェックします。

- インストールされているプログラムがアクティブスキャンをサポートしない場合、HostScan/Secure Firewall ポスチャはそのソフトウェアの存在をレポートします。DAP システムは、そのプログラムを指定する DAP レコードを選択します。
- インストールされているプログラムがアクティブスキャンをサポートしており、そのプログラムでアクティブスキャンがイネーブルになっている場合、HostScan/Secure Firewall ポスチャはそのソフトウェアの存在をレポートします。この場合も、セキュリティアプライアンスは、そのプログラムを指定する DAP レコードを選択します。
- インストールされているプログラムがアクティブスキャンをサポートしており、そのプログラムでアクティブスキャンが無効になっている場合、HostScan/Secure Firewall ポスチャはそのソフトウェアの存在を無視します。セキュリティアプライアンスは、そのプログラムを指定する DAP レコードを選択しません。さらに、プログラムがインストールされている場合でも、DAP に関する多数の情報が含まれる **debug trace** コマンドの出力にはプログラムの存在が示されません。

（注） HostScan 4.3.x から HostScan 4.6.x 以降にアップグレードする場合は、アップグレードの前に、既存の AV/AS/FW エンドポイント属性を対応する代替 AM/FW エンドポイント属性に移行する必要があります。アップグレードおよび移行の完全な手順については、『AnyConnect HostScan 4.3.x to 4.6.x Migration Guide』を参照してください。

エンドポイント属性の定義

次に、DAP で使用できるエンドポイント選択属性を示します。[Attribute Name] フィールドは、LUA 論理式での各属性名の入力方法を示しており、[Dynamic Access Policy Selection Criteria] ペインの [Advanced] 領域で使用します。*label* 変数は、アプリケーション、ファイル名、プロセス、またはレジストリ エントリを示します。

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
マルウェア対策	endpoint.am["*label*"].exists	Host ScanSecure Firewall ポスチャ	true	—	マルウェア対策プログラムが存在する
	endpoint.am["*label*"].version		string	32	Version
	endpoint.am["*label*"].description		string	128	マルウェア対策の説明
	endpoint.am["*label*"].lastupdate		整数	—	マルウェア対策定義を更新してからの経過時間（秒）
Personal Firewall	endpoint.pfw["*label*"].exists	Host ScanSecure Firewall ポスチャ	true	—	パーソナルファイアウォールが存在する
	endpoint.pfw["*label*"].version		string	string	Version
	endpoint.pfw["*label*"].description		string	128	パーソナルファイアウォールの説明

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
AnyConnect（HostScan/Secure Firewall ポスチャは不要）	endpoint.anyconnect.clientversion	エンドポイント	version	—	セキュアクライアント バージョン
	endpoint.anyconnect.platform		string	—	セキュアクライアントがインストールされているオペレーティングシステム
	endpoint.anyconnect.platformversion		version	64	セキュアクライアントがインストールされているオペレーティングシステムのバージョン
	endpoint.anyconnect.devicetype		string	64	セキュアクライアントがインストールされているモバイルデバイスのタイプ
	endpoint.anyconnect.deviceuniqueid			64	セキュアクライアントがインストールされているモバイルデバイスの一意の ID
	endpoint.anyconnect.macaddress		string	—	セキュアクライアントがインストールされているデバイスの MAC アドレス。 フォーマットは xx-xx-xx-xx-xx-xx であることが必要です。x は有効な 16 進数文字です。
アプリケーション	endpoint.application.clienttype	アプリケーション	string	—	クライアント タイプ： CLIENTLESS ANYCONNECT IPSEC L2TP

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
デバイス	endpoint.device. hostname	エンドポイント	string	64	ホスト名のみ。FQDN ではありません
	endpoint.device.MAC		string	—	ネットワーク インターフェイス カードの MAC アドレス。1 つのエントリにつき MAC アドレスは 1 つだけです フォーマットは xxxx.xxxx.xxxx であることが必要です。x は 16 進数文字です。
	endpoint.device.id		string	64	BIOS シリアル番号。数値フォーマットは、製造業者固有です。フォーマット要件はありません
	endpoint.device.port		string	—	リスニング状態の TCP ポート 1 回線ごとに 1 つのポートを定義できます 1 ～ 65535 の範囲の整数
	endpoint.device. protection_version		string	64	実行される HostScan/Secure Firewall ポスチャイメージのバージョン
	endpoint.device. protection_extension		string	64	Endpoint Assessment（OPSWAT）のバージョン

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
ファイル	endpoint.file["*label*"].exists		true	—	ファイルが存在する
	endpoint.file[“label”].endpointid				
	endpoint.file["*label*"].lastmodified		整数	—	ファイルが最後に変更されてからの経過時間（秒）
	endpoint.file["*label*"].crc.32		整数	—	ファイルの CRC32 ハッシュ
NAC	endpoint.nac.status	NAC	string	—	ユーザー定義ステータス ストリング
オペレーティング システム	endpoint.os.version		string	32	オペレーティング システム
	endpoint.os.servicepack		整数	—	Windows のサービス パック
ポリシー（Policy）	endpoint.policy.location		string	64	
プロセス	endpoint.process["*label*"].exists		true	—	プロセスが存在する
	endpoint.process["*label*"].path		string	255	プロセスのフルパス
Registry	endpoint.registry["*label*"].type		*dword string*	—	dword
	endpoint.registry["*label*"].value		string	255	レジストリ エントリの値
VLAN	endoint.vlan.type	CNA	string	—	VLAN タイプ： ACCESS AUTH ERROR GUEST QUARANTINE ERROR STATIC TIMEOUT

LUA を使用した DAP における追加の DAP 選択基準の作成

このセクションでは、AAA またはエンドポイント属性の論理式の作成方法について説明します。これを行うには、LUA に関する高度な知識が必要です。LUA のプログラミングの詳細情報については、http://www.lua.org/manual/5.1/manual.html を参照してください。

[Advanced] フィールドに、AAA またはエンドポイント選択論理演算を表す自由形式の LUA テキストを入力します。ASDM は、ここで入力されたテキストを検証せず、テキストを DAP ポリシー ファイルにコピーするだけです。処理は ASA によって行われ、解析不能な式は破棄されます。

このオプションは、上の説明にある AAA およびエンドポイントの属性領域で指定可能な基準以外の選択基準を追加する場合に有効です。たとえば、指定された条件のいずれかを満たす、すべてを満たす、またはいずれも満たさない AAA 属性を使用するように ASA を設定できます。エンドポイント属性は累積され、そのすべてを満たす必要があります。セキュリティ アプライアンスが任意のエンドポイント属性を使用できるようにするには、LUA で適切な論理式を作成し、ここでその式を入力する必要があります。

次のセクションでは、LUA EVAL 式作成の詳細と例を示します。

- LUA EVAL 式を作成する構文 （27 ページ）
- DAP EVAL 式の例 （32 ページ）
- 追加の LUA 関数 （29 ページ）

LUA EVAL 式を作成する構文

（注） [Advanced] モードを使用する必要がある場合は、プログラムを直接的に検証することが可能になり、明確になるため、できるだけ EVAL 式を使用することをお勧めします。

EVAL(<*attribute*> , <comparison>, {<*value*> | <*attribute*>}, [<type>])

<attribute>	AAA 属性または Cisco Secure Desktop から返された属性。属性の定義については、エンドポイント属性の定義 （23 ページ） を参照してください。

<comparison>	次の文字列のいずれか（引用符が必要）	
	“EQ”	等しい
	“NE”	等しくない
	“LT”	より小さい
	“GT”	より大きい
	“LE”	以下
	“GE”	以上
<value>	引用符で囲まれ、属性と比較する値を含む文字列	
<type>	次の文字列のいずれか（引用符が必要）	
	“string”	大文字、小文字を区別する文字列の比較
	“”	大文字、小文字を区別しない文字列の比較
	“integer”	数値比較で、文字列値を数値に変換
	“hex”	16 進数を用いた数値比較で、16 進数の文字列を 16 進数に変換
	“version”	X.Y.Z. 形式（X、Y、Z は数字）のバージョンを比較

HostScan 4.6（およびそれ以降）および Secure Firewall ポスチャバージョン 5 の LUA 手順

'ANY' のウイルス対策（endpoint.am）用 LUA スクリプト（最終更新済み）

次の LUA スクリプトを使用して、'ANY' のウイルス対策製品/ベンダー（endpoint.am）を確認します。異なる最終更新の間隔に対応するため、修正が適用される場合があります。次の例は、30 日（2592000 秒と記載）以内に実行されたものとする最終更新の方法を示しています。

```
assert(function()
  for k,v in pairs(endpoint.am) do
    if(EVAL(v.activescan, "EQ", "ok", "string")and EVAL (v.lastupdate, "LT", "2592000",
 "integer"))
     then
              return true
         end
  end
  return false
end)()
```

'ANY' のパーソナル ファイアウォール用 LUA スクリプト

次の LUA スクリプトを使用して、'ANY' のファイアウォール製品/ベンダー（endpoint.pfw）を確認します。

```
assert(function()
    for k,v in pairs(endpoint.pfw) do
         if (EVAL(v.enabled, "EQ", "ok", "string")) then
              return true
         end
    end
    return false
end)()
```

追加の LUA 関数

ダイナミック アクセス ポリシーで作業している場合、一致基準に高度な柔軟性が必要とされることが考えられます。たとえば、以下に従い別の DAP を適用しなければならない場合があります。

- CheckAndMsg は、DAP がコールするように設定可能な LUA 関数です。条件に基づきユーザー メッセージを生成します。
- 組織ユニット（OU）またはユーザー オブジェクトの他の階層のレベル。
- 命名規則に従ったグループ名に多くの一致候補がある場合、ワイルドカードの使用が必要になることがあります。

ASDM の [DAP] ペイン内の [Advanced] セクションで LUA 論理式を作成し、この柔軟性を実現できます。

DAP CheckAndMsg 関数

ASA は、LUA CheckAndMsg 関数を含む DAP レコードが選択され、それによって接続が終了する結果になる場合にのみ、ユーザーにメッセージを表示します。

CheckAndMsg 関数の構文は以下の通りです。

```
CheckAndMsg(value, "<message string if value is true>", "<message string if value if
false>")
```

CheckAndMsg 関数の作成時には、以下の点に注意してください。

- CheckAndMsg は、最初の引数として渡された値を返します。
- 文字列比較を使用したくない場合、EVAL 関数を最初の引数として使用してください。次に例を示します。

```
(CheckAndMsg((EVAL(...)) , "true msg", "false msg"))
```

CheckandMsg は EVAL 関数の結果を返し、セキュリティ アプライアンスはその結果を使用して、DAP レコードを選択すべきかどうかを判断します。レコードが選択された結果、ターミネーションとなった場合、セキュリティアプライアンスは適切なメッセージを表示します。

OU ベースの照合の例

DAP は、論理式で LDAP サーバーから返される多数の属性を使用できます。DAP トレースの項で出力例を参照するか、debug dap トレースを実行してください。

LDAP サーバーはユーザーの認定者名（DN）を返します。これは、ディレクトリ内のどの部分にユーザー オブジェクトがあるかを暗黙的に示します。たとえば、ユーザーの DN が CN=Example User、OU=Admins、dc=cisco、dc=com である場合、このユーザーは OU=Admins,dc=cisco,dc=com に存在します。すべての管理者がこの OU（または、このレベル以下のコンテナ）に存在する場合、以下のように、この基準に一致する論理式を使用できます。

```
assert(function()
   if ( (type(aaa.ldap.distinguishedName) == "string") and
        (string.find(aaa.ldap.distinguishedName, "OU=Admins,dc=cisco,dc=com$") ~= nil)
) then
       return true
   end
   return false
end)()
```

この例では、string.find 関数で正規表現を使用できます。この文字列を distinguishedName フィールドの最後にアンカーするには、文字列の最後に $ を使用します。

グループ メンバーシップの例

AD グループ メンバーシップのパターン照合のために、基本論理式を作成できます。ユーザーが複数のグループのメンバーであることが考えられるため、DAP は LDAP サーバーからの応答を表内の別々のエントリへと解析します。以下を実行するには、高度な機能が必要です。

- memberOf フィールドを文字列として比較する（ユーザーが 1 つのグループだけに所属している場合）。
- 返されたデータが「table」タイプである場合、返されたそれぞれの memberOf フィールドを繰り返し処理する。

そのために記述し、テストした関数を以下に示します。この例では、ユーザーが「-stu」で終わるいずれかのグループのメンバーである場合、この DAP に一致します。

```
assert(function()
   local pattern = "-stu$"
   local attribute = aaa.ldap.memberOf
   if ((type(attribute) == "string") and
       (string.find(attribute, pattern) ~= nil)) then
       return true
   elseif (type(attribute) == "table") then
       local k, v
```

```
       for k, v in pairs(attribute) do
           if (string.find(v, pattern) ~= nil) then
               return true
           end
       end
   end
   return false
end)()
```

アクセス拒否の例

マルウェア対策プログラムが存在しない場合のアクセスを拒否するために、次の関数を使用できます。ターミネーションを実行するためのアクションが設定されているDAPで使用します。

```
assert(
    function()
for k,v in pairs(endpoint.am) do

        if (EVAL(v.exists, "EQ", "true", "string")) then

            return false

        end
    end
    return CheckAndMsg(true, "Please install antimalware software before connecting.",
nil)
end)()
```

マルウェア対策プログラムがないユーザーがログインしようとすると、DAPは次のメッセージを表示します。

```
Please install antimalware software before connecting.
```

マルチ証明書認証の例

DAP ルールで複数の証明書認証を使用して、ワイルドカード発行者の CN を定義できます。

2 つの異なる認証局（abc.cisco.com と xyz.cisco.com など）によって 2 つの異なるマシンに発行された2つの証明書を設定した場合、DAPルールには、発行者CNが*.cisco.comまたはcisco.comである複数の証明書認証の条件が必要です。

次の関数を使用して、ユーザーおよびマシンの証明書にワイルドカード issuer_cn cisco.com を使用して証明書の DAP ルールを定義できます。

```
assert(
 function()
  if ((string.find(endpoint.cert[1].issuer.cn[0], "cisco.com") ~= nil) and
   (string.find(endpoint.cert[2].issuer.cn[0], "cisco.com") ~= nil)) then
     return true;
 end
 return false;
end)()
```

DAP EVAL 式の例

LUA で論理式を作成する場合は、次の例を参考にしてください。

説明	例
Windows 10 用エンドポイント LUA チェック	`(EVAL(endpoint.os.version,"EQ","Windows 10","string"))`
CLIENTLESS または CVC クライアントタイプに一致するかどうかのエンドポイント LUA チェック。	`(EVAL(endpoint.application.clienttype,"EQ","CLIENTLESS") or EVAL(endpoint.application.clienttype, "EQ","CVC"))`
単一マルウェア対策プログラム Symantec Enterprise Protection がユーザーの PC にインストールされているかどうかのエンドポイント LUA チェック。インストールされていない場合はメッセージを表示します。	`(CheckAndMsg(EVAL(endpoint.am["538"].description,"NE","Symantec Endpoint Protection","string"),"Symantec Endpoint Protection was not found on your computer", nil))`
McAfee Endpoint Protection バージョン 10 から 10.5.3 およびバージョン 10.6 以降用のエンドポイント LUA チェック。	`(EVAL(endpoint.am["1637"].version,"GE","10","version") and EVAL(endpoint.am["1637"].version,"LT","10.5.4","version") or EVAL(endpoint.am["1637"].version,"GE","10.6","version"))`
McAfee マルウェア対策定義が過去 10 日（864000 秒）以内に更新されたかどうかのエンドポイント LUA チェック。更新が必要な場合はメッセージを表示します。	`(CheckAndMsg(EVAL(endpoint.am["1637"].lastupdate,"GT","864000","integer"),"Update needed! Please wait for McAfee to load the latest dat file.", nil))`
debug dap trace で `endpoint.os.windows.hotfix["KB923414"] = "true";` が返された後に特定のホットフィックスがあるかどうかのチェック。	`(CheckAndMsg(EVAL(endpoint.os.windows.hotfix["KB923414"],"NE","true"), "The required hotfix is not installed on your PC.",nil))`

マルウェア対策プログラムのチェックとメッセージの表示

マルウェア対策ソフトウェアにより、エンドユーザーが問題に気づいて修正できるようにメッセージを設定できます。アクセスが許可された場合、ASA はポータル ページの DAP 評価プロセスで生成されたすべてのメッセージを表示します。アクセスが拒否された場合、ASAは「ター

ミネーション」状態の原因となったすべてのメッセージを DAP から収集して、ブラウザのログイン ページに表示します。

次の例は、この機能を使用して Symantec Endpoint Protection のステータスをチェックする方法を示します。

1. 次の LUA 式をコピーし、[Add/Edit Dynamic Access Policy] ペインの [Advanced] フィールドに貼り付けます（右端にある二重矢印をクリックして、フィールドを展開します）。

```
(CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint
Protection","string") and EVAL(endpoint.am["538"].activescan,"NE","ok","string")
"Symantec Endpoint Protection is disabled. You must enable before being granted
access", nil))
```

2. 同じ [Advanced] フィールドで、[OR] ボタンをクリックします。
3. 下の [Access Attributes] セクションの一番左の [Action] タブで、[Terminate] をクリックします。
4. Symantec Endpoint Protection がインストールされているものの無効になっている PC から接続します。想定される結果は、接続は許可されず、ユーザーに次のメッセージが表示されるというものです。「Symantec Endpoint Protection is disabled. You must enable before being granted access」。

マルウェア対策プログラムと 2 日以上経過した定義のチェック

この例では、Symantec または McAfee のマルウェア対策プログラムが存在するかどうか、また、ウイルス定義が 2 日（172,800 秒）以内のものであるかどうかを確認します。定義が 2 日以上経過している場合、ASA はセッションを終了し、メッセージと修正用リンクを表示します。このタスクを完了するには、次の手順を実行します。

1. 次の LUA 式をコピーし、[Add/Edit Dynamic Access Policy] ペインの [Advanced] フィールドに貼り付けます。

```
(CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint
Protection","string") and EVAL(endpoint.am["538"].lastupdate,"GT","172800","integer"),
 "Symantec Endpoint Protection Virus Definitions are Out of Date. You must run
LiveUpdate before being granted access", nil)) or
(CheckAndMsg(EVAL(endpoint.am["1637"].description,"EQ","McAfee Endpoint
Security","string") and EVAL(endpoint.am["1637"].lastupdate,"GT","172800","integer"),
 "McAfee Endpoint Security Virus Definitions are Out of Date. You must update your
McAfee Virus Definitions before being granted access", nil))
```

2. 同じ [Advanced] フィールドで、[AND] をクリックします。
3. 下の [Access Attributes] セクションの一番左の [Action] タブで、[Terminate] をクリックします。
4. Symantec または McAfee のマルウェア対策プログラムがインストールされており、バージョンが 2 日以上前のものである PC から接続します。

   結果として、接続は許可されず、ユーザーに「virus definitions are out of date」というメッセージが表示されることが予測されます。

DAP アクセスと許可ポリシー属性の設定

各タブをクリックして、タブ内のフィールドを設定します。

手順

ステップ 1 特定の接続またはセッションに適用される特別な処理を指定するには、[Action] タブを選択します。

- [Continue]：（デフォルト）セッションにアクセス ポリシー属性を適用します。
- [Quarantine]：検疫を使用すると、VPN 経由ですでにトンネルを確立している特定のクライアントを制限できます。ASAは、制限付きACLをセッションに適用して制限付きグループを形成します。この基になるのは、選択された DAP レコードです。エンドポイントが管理面で定義されているポリシーに準拠していない場合でも、ユーザーはサービスにアクセスして修復できますが、ユーザーに制限がかけられます。修復後、ユーザーは再接続できます。この再接続により、新しいポスチャアセスメントが起動されます。このアセスメントに合格すると、接続されます。このパラメータを使用するには、セキュアクライアント機能をサポートしている セキュアクライアント リリースが必要です。
- [Terminate]：セッションを終了します。
- [User Message]：この DAP レコードが選択されるときに、ポータル ページに表示するテキスト メッセージを入力します。最大 490 文字を入力できます。ユーザー メッセージは、黄色のオーブとして表示されます。ユーザーがログインすると、メッセージは3回点滅してから静止します。数件の DAP レコードが選択され、それぞれにユーザー メッセージがある場合は、ユーザー メッセージがすべて表示されます。

  URL やその他の埋め込みテキストを含めることができます。この場合は、正しい HTML タグを使用する必要があります。例：すべてのコントラクタは、ご使用のマルウェア対策ソフトウェアのアップグレード手順について、Instructions を参照してください。

ステップ 2 [Network ACL Filters] タブを選択し、この DAP レコードに適用されるネットワーク ACL を設定します。

DAP の ACL には、許可ルールまたは拒否ルールを含めることができますが、両方を含めることはできません。ACLに許可ルールと拒否ルールの両方が含まれている場合、ASAはそのACLを拒否します。

- [Network ACL] ドロップダウン リスト：この DAP レコードに追加する、すでに設定済みのネットワーク ACL を選択します。ACL には、許可ルールと拒否ルールの任意の組み合わせを指定できます。このフィールドは、IPv4 および IPv6 ネットワーク トラフィックのアクセス ルールを定義できる統合 ACL をサポートしています。
- [Manage]：ネットワーク ACL を追加、編集、および削除するときにクリックします。

- [Network ACL] リスト：この DAP レコードのネットワーク ACL が表示されます。
- [Add]：ドロップダウン リストで選択したネットワーク ACL が右側の [Network ACLs] リストに追加されます。
- [Delete]：クリックすると、強調表示されているネットワーク ACL が [Network ACLs] リストから削除されます。ASA から ACL を削除するには、まず DAP レコードからその ACL を削除する必要があります。

ステップ 3 [Web-Type ACL Filters (clientless)] タブを選択し、この DAP レコードに適用される Web タイプ ACL を設定します。DAP の ACL には、許可または拒否ルールだけを含めることができます。ACL に許可ルールと拒否ルールの両方が含まれている場合、ASA はその ACL を拒否します。

- [Web-Type ACL] ドロップダウン リスト：この DAP レコードに追加する、設定済みの Web-type ACL を選択します。ACL には、許可ルールと拒否ルールの任意の組み合わせを指定できます。
- [Manage]：Web タイプ ACL を追加、編集、削除するときにクリックします。
- [Web-Type ACL] リスト：この DAP レコードの Web-type ACL が表示されます。
- [Add]：ドロップダウン リストで選択した Web タイプ ACL が右側の [Web-Type ACLs] リストに追加されます。
- [Delete]：クリックすると、Web-type ACL の 1 つが [Web-Type ACLs] リストから削除されます。ASA から ACL を削除するには、まず DAP レコードからその ACL を削除する必要があります。

ステップ 4 [Functions] タブを選択し、ファイル サーバー エントリとブラウジング、HTTP プロキシ、および DAP レコードの URL エントリを設定します。

- [File Server Browsing]：ファイル サーバーまたは共有機能の CIFS ブラウジングをイネーブルまたはディセーブルにします。

  ブラウズには、NBNS（マスター ブラウザまたは WINS）が必要です。NBNS に障害が発生した場合や、NBNS が設定されていない場合は、DNS を使用します。CIFS ブラウズ機能では、国際化がサポートされていません。
- [File Server Entry]：ポータル ページでユーザーがファイル サーバーのパスおよび名前を入力できるようにするかどうかを設定します。イネーブルになっている場合、ポータル ページにファイル サーバー エントリのドロワが配置されます。ユーザーは、Windows ファイルへのパス名を直接入力できます。ユーザーは、ファイルをダウンロード、編集、削除、名前変更、および移動できます。また、ファイルおよびフォルダを追加することもできます。適用可能な Windows サーバーでユーザー アクセスに対して共有を設定する必要もあります。ネットワークの要件によっては、ユーザーがファイルへのアクセス前に認証を受ける必要があることもあります。
- [HTTP Proxy]：クライアントへの HTTP アプレット プロキシの転送に関与します。このプロキシは、適切なコンテンツ変換に干渉するテクノロジー（Java、ActiveX、Flash など）に対して有用です。このプロキシによって、セキュリティ アプライアンスの使用を継続し

ながら、マングリングを回避できます。転送されたプロキシは、自動的にブラウザの古いプロキシ コンフィギュレーションを変更して、すべての HTTP および HTTPS 要求を新しいプロキシ コンフィギュレーションにリダイレクトします。HTTP アプレット プロキシでは、HTML、CSS、JavaScript、VBScript、ActiveX、Java など、ほとんどすべてのクライアント側テクノロジーがサポートされています。サポートされているブラウザは、Microsoft Internet Explorer だけです。

- [URL Entry]：ポータル ページでユーザーが HTTP/HTTPS URL を入力できるようにするかどうかを設定します。この機能がイネーブルになっている場合、ユーザーは URL エントリ ボックスに Web アドレスを入力できます。

SSL VPN を使用しても、すべてのサイトとの通信が必ずしもセキュアになるとはかぎりません。SSL VPN は、企業ネットワーク上のリモート ユーザーの PC やワークステーションと ASA との間のデータ転送のセキュリティを保証するものです。したがって、ユーザーが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるリソース）にアクセスする場合、企業の ASA から目的の Web サーバーまでの通信はセキュアではありません。

クライアントレス VPN 接続では、ASA はエンド ユーザーの Web ブラウザとターゲット Web サーバーとの間のプロキシとして機能します。ユーザーが SSL 対応 Web サーバーに接続すると、ASA はセキュアな接続を確立し、サーバーの SSL 証明書を検証します。エンド ユーザー ブラウザでは提示された証明書を受信しないため、証明書を調査して検証することはできません。SSL VPN の現在の実装では、期限切れになった証明書を提示するサイトとの通信は許可されません。また、ASA は信頼できる CA 証明書の検証も実行しません。このため、ユーザーは、SSL 対応の Web サーバーと通信する前に、そのサーバーにより提示された証明書を分析することはできません。

ユーザーのインターネット アクセスを制限するには、[Disable for the URL Entry] フィールドを選択します。これにより、SSL VPN ユーザーがクライアントレス VPN 接続中に Web サーフィンできないようにします。

- [Unchanged]：（デフォルト）クリックすると、このセッションに適用されるグループ ポリシーからの値が使用されます。
- [Enable/Disable]：機能をイネーブルにするかディセーブルにするかを指定します。
- [Auto-start]：クリックすると HTTP プロキシがイネーブルになり、これらの機能に関連付けられたアプレットが DAP レコードによって自動的に起動するようになります。

ステップ 5 [Port Forwarding Lists] タブを選択し、ユーザー セッションのポート転送リストを設定します。

ポート転送によりグループ内のリモート ユーザーは、既知の固定 TCP/IP ポートで通信するクライアント/サーバー アプリケーションにアクセスできます。リモート ユーザーは、ローカル PC にインストールされたクライアント アプリケーションを使用して、そのアプリケーションをサポートするリモート サーバーに安全にアクセスできます。シスコでは、Windows Terminal Services、Telnet、Secure FTP（FTP over SSH）、Perforce、Outlook Express、および Lotus Notes についてテストしています。その他の TCP ベースのアプリケーションの一部も機能すると考えられますが、シスコではテストしていません。

（注）

ポート転送は、一部の SSL/TLS バージョンでは使用できません。

注意
ポート転送（アプリケーション アクセス）およびデジタル証明書をサポートするために、リモート コンピュータに Sun Microsystems Java ランタイム環境（JRE）がインストールされていることを確認します。

- [Port Forwarding]：この DAP レコードに適用されるポート転送リストのオプションを選択します。このフィールドのその他の属性は、[Port Forwarding] を [Enable] または [Auto-start] に設定した場合にだけイネーブルになります。
- [Unchanged]：クリックすると、属性が実行コンフィギュレーションから削除されます。
- [Enable/Disable]：ポート転送をイネーブルにするかディセーブルにするかを指定します。
- [Auto-start]：クリックするとポート転送がイネーブルになり、DAP レコードのポート転送リストに関連付けられたポート転送アプレットが自動的に起動するようになります。
- [Port Forwarding List] ドロップダウン リスト：DAP レコードに追加する、設定済みのポート転送リストを選択します。
- **[New...]**：新規のポート転送リストを設定するときにクリックします。
- [Port Forwarding Lists]（ラベルなし）：DAP レコードのポート転送リストが表示されます。
- [Add]：クリックすると、ドロップダウン リストで選択したポート転送リストが右側のポート転送リストに追加されます。
- [Delete]：クリックすると、選択されているポート転送リストがポート転送リストから削除されます。 ASA からポート転送リストを削除するには、まず DAP レコードからそのリストを削除する必要があります。

ステップ 6 [Bookmarks] タブを選択し、特定のユーザー セッション URL のブックマークを設定します。

- [Enable bookmarks]：クリックするとイネーブルになります。 このチェックボックスがオフのときは、接続のポータル ページにブックマークは表示されません。
- [Bookmark] ドロップダウン リスト：DAP レコードに追加する、設定済みのブックマークを選択します。
- **[Manage...]**：ブックマークを追加、インポート、エクスポート、削除するときにクリックします。
- **[Bookmarks]**（ラベルなし）：この DAP レコードの URL リストが表示されます。
- [Add>>]：クリックすると、ドロップダウン リストで選択したブックマークが右側の URL 領域に追加されます。
- [Delete]：クリックすると、選択されているブックマークが URL リスト領域から削除されます。ASA からブックマークを削除するには、まず DAP レコードからそのブックマークを削除する必要があります。

ステップ 7 [Access Method] タブを選択し、許可するリモート アクセスのタイプを設定します。

- [Unchanged]：現在のリモート アクセス方式を引き続き使用します。
- **セキュアクライアント**：Cisco Secure Client AnyConnect VPN クライアントの AnyConnect VPN モジュールを使用して接続する

  .
- [Web-Portal]：クライアントレス VPN で接続します。
- **Both-default-Web-Portal**：クライアントレスまたはセキュアクライアントを介して接続します。デフォルトはクライアントレスです。
- **Both-default-セキュアクライアント**：クライアントレスまたはセキュアクライアントを介して接続します。セキュアクライアントのデフォルトはクライアントレスです。

ステップ 8 [**セキュアクライアント**] タブを選択し、Always-on VPN フラグのステータスを選択します。

- Always-On VPN for セキュアクライアント：セキュアクライアント サービスプロファイル内の Always-on VPN フラグ設定を未変更にするか、ディセーブルにするか、セキュアクライアント プロファイル設定を使用するかを指定します。

  このパラメータを使用するには、Cisco Web セキュリティ アプライアンスのリリースが、Cisco Secure クライアントの AnyConnect VPN モジュールに対してセキュア モビリティ ソリューションライセンシングをサポートしている必要があります。また、セキュアクライアント のリリースが、「セキュア モビリティ ソリューション」の機能をサポートしている必要もあります。詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

ステップ 9 [セキュアクライアント カスタム属性（AnyConnect Client Custom Attributes）] タブを選択し、定義済みのカスタム属性を表示して、このポリシーに関連付けます。また、カスタム属性を定義してから、それらをこのポリシーに関連付けることもできます。

カスタム属性はセキュアクライアントに送信され、アップグレードの延期などの機能を設定するために使用されます。カスタム属性にはタイプと名前付きの値があります。まず属性のタイプを定義した後、このタイプの名前付きの値を 1 つ以上定義できます。機能に対して設定する固有のカスタム属性の詳細については、使用しているセキュアクライアントリリースの『*Cisco Secure Client Administrator Guide*』を参照してください。

カスタム属性は、[設定（Configuration）] > [リモートアクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [詳細設定（Advanced）] > [セキュアクライアントカスタム属性（Custom Attributes）] および [セキュアクライアントカスタム属性名（Custom Attribute Names）] で事前に定義できます。事前に定義したカスタム属性は、ダイナミック アクセス ポリシーとグループ ポリシーの両方で使用されます。

DAP を使用した SAML 認証の設定

外部サーバー（RADIUS またはLDAP）に依存して認可属性を取得することなく、DAP を使用して SAML 認可およびグループポリシーの選択を設定できます。

SAML ID プロバイダーは、認証アサーションに加えて認可属性を送信するように設定できます。ASA の SAML サービス プロバイダー コンポーネントは、SAML アサーションを解釈し、受信したアサーションに基づいて認可またはグループポリシーの選択を行います。アサーション属性は、ASDM で設定された DAP ルールを使用して処理されます。

グループポリシー属性は、属性名 **cisco_group_policy** を使用する必要があります。この属性は、設定されている DAP に依存しません。ただし、DAP が設定されている場合は、DAP ポリシーの一部として使用できます。

グループポリシーの選択

cisco_group_policy という名前の属性が受信されると、対応する値を使用して接続 group-policy が選択されます。

接続が確立されると、複数のソースからグループポリシー情報が取得され、それらが組み合わされて、接続に適用される有効な group-policy が作成されます。

受信したグループポリシー情報を組み合わせると、次のシナリオが考えられます。

SAML 認証で受信したグループポリシー、承認が設定されていません

このシナリオでは、有効なグループポリシーは、優先順位の降順で次のように決定されます。

1. SAML 属性で指定されたグループポリシー。
2. トンネルグループで指定されたグループポリシー。
3. デフォルトのグループポリシー。

SAML 認証で受信したグループポリシー、承認が設定されています

このシナリオでは、有効なグループポリシーは、優先順位の降順で次のように決定されます。

1. 許可属性で指定されたグループポリシー。
2. ユーザーグループポリシー：存在する場合、許可サーバーから返された値を使用します。
3. ユーザーグループポリシー：SAML 属性で返された値を使用します。
4. トンネルグループで指定されたグループポリシー。
5. デフォルトのグループポリシー。

手順

ステップ 1 ASDM では、**[設定（Configuration）] > [リモートアクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [ダイナミックアクセスポリシー（Dynamic Access Policies）] > [ダイナミックポリシーの追加/編集（Add/Edit Dynamic Access Policy）]**を選択します。

ステップ 2 AAA 属性の選択領域で、[追加（Add）] をクリックします。

a) [AAA属性タイプ（AAA Attribute Type）] ドロップダウンから、[SAML] を選択します。

b) 属性 *ID*として **memberOf** を指定します。

c) *memberOf* 属性の**値**を入力するか、AD サーバーグループが設定されている場合は [ADグループの取得（Get AD Group）] をクリックします。

追加の AD サーバーグループを設定するには、**[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [AAA/ローカルユーザー（AAA/Local Users）] > [AAA サーバーグループ（AAA Server Groups）]**に移動します。

グループポリシー選択属性を構成するには、必要に応じて、同じ DAP ポリシーまたは別の DAP ポリシーで次の設定を選択します。

- [AAA属性タイプ（AAA Attribute Type）] : SAML
- [属性 ID（Attribute ID）] : cisco_group_policy
- [値（Value）] : グループポリシー名

ステップ 3 [OK] をクリックします。

ステップ 4 [OK] をクリックして、DAP ポリシーを保存します。

DAP トレースの実行

DAP トレースを実行すると、すべての接続済みデバイスの DAP エンドポイント属性が表示されます。

手順

ステップ 1 SSH ターミナルから ASA にログオンして特権 EXEC モードを開始します。

ASA の特権 EXEC モードでは、表示されるプロンプトは `hostname#` となります。

ステップ 2 DAP デバッグをイネーブルにします。セッションのすべての DAP 属性がターミナル ウィンドウに表示されます。

```
hostname# debug dap trace
endpoint.anyconnect.clientversion="0.16.0021";
endpoint.anyconnect.platform="apple-ios";
endpoint.anyconnect.platformversion="4.1";
endpoint.anyconnect.devicetype="iPhone1,2";
endpoint.anyconnect.deviceuniqueid="dd13ce3547f2fa1b2c3d4e5f6g7h8i9j0fa03f75";
```

ステップ 3 （任意） DAP トレースの出力を検索するには、コマンドの出力をシステム ログに送ります。ASA でのロギングの詳細については、『*Cisco ASA Series General Operations ASDM Configuration Guide*』の「*Configure Logging*」を参照してください。

DAP の例

DAP を使用したネットワーク リソースの定義

この例は、ユーザーまたはグループのネットワーク リソースを定義する方法として、ダイナミック アクセス ポリシーを設定する方法を示しています。Trusted_VPN_Access という名前の DAP ポリシーは、 Cisco Secure Client のクライアントレス VPN アクセスと AnyConnect VPN モジュールアクセスを許可します。Untrusted_VPN_Access という名前のポリシーは、クライアントレス VPN アクセスだけを許可します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Dynamic Access Policies]** > **[Add/Edit Dynamic Access Policy]** > **[Endpoint]** に移動します。

ステップ 2 各ポリシーの次の属性を設定します。

属性	Trusted_VPN_Access	Untrusted_VPN_Access
Endpoint Attribute Type Policy	信頼できる	信頼できない
Endpoint Attribute Process	ieexplore.exe	—
Advanced Endpoint Assessment	AntiVirus= McAfee Attribute	
CSD Location	信頼できる	信頼できない
LDAP memberOf	Engineering、Managers	ベンダー

属性	Trusted_VPN_Access	Untrusted_VPN_Access
ACL		Web-Type ACL
アクセス	セキュアクライアントおよび Web ポータル	Web Portal

DAP を使用した WebVPN ACL の適用

DAP では、Network ACLs（IPsec およびセキュアクライアント の場合）、URL リスト、および Functions を含め、アクセスポリシー属性のサブセットを直接適用できます。グループ ポリシーが適用されるバナーまたはスプリット トンネル リストなどには、直接適用できません。[Add/Edit Dynamic Access Policy] ペインの [Access Policy Attributes] タブには、DAP が直接適用される属性の完全なメニューが表示されます。

Active Directory/LDAP は、ユーザー グループ ポリシー メンバーシップをユーザー エントリの「memberOf」属性として保存します。AD グループ内のユーザー（memberOf）= ASA が設定済み Web タイプ ACL を適用する Engineering となるように、DAP を定義します。

手順

ステップ 1 ASDM で、[Add AAA Attributes] ペインに移動します（**[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Dynamic Access Policies]** > **[Add/Edit Dynamic Access Policy]** > **[AAA Attributes section]** > **[Add AAA Attribute]**）。

ステップ 2 AAA 属性タイプとしては、ドロップダウン リストを使用して [LDAP] を選択します。

ステップ 3 [Attribute ID] フィールドに、ここに示されるとおり「memberOf」と入力します。大文字と小文字の区別は重要です。

ステップ 4 [Value] フィールドで、ドロップダウン リストを使用して [=] を選択し、隣のフィールドに「Engineering」と入力します。

ステップ 5 ペインの [Access Policy Attributes] 領域で、[Web-Type ACL Filters] タブをクリックします。

ステップ 6 [Web-Type ACL] ドロップダウン リストを使用して、AD グループ（memberOf）= Engineering のユーザーに適用する ACL を選択します。

DAP による CSD チェックの強制とポリシーの適用

この例では、ユーザーが 2 つの特定 AD/LDAP グループ（Engineering および Employees）と 1 つの特定 ASA トンネル グループに属することをチェックする DAP を作成します。その後、ACL をユーザーに適用します。

DAP が適用される ACL により、リソースへのアクセスを制御します。それらの ACL は、ASA のグループ ポリシーで定義されるどの ACL よりも優先されます。また ASA は、スプリットトンネリング リスト、バナー、DNS など、DAP で定義または制御されない要素に通常の AAA グループ ポリシー継承ルールと属性を適用します。

手順

ステップ 1 ASDM で、[Add AAA Attributes] ペインに移動します（**[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Dynamic Access Policies]** > **[Add/Edit Dynamic Access Policy]** > **[AAA Attributes section]** > **[Add AAA Attribute]**）。

ステップ 2 AAA 属性タイプとしては、ドロップダウン リストを使用して [LDAP] を選択します。

ステップ 3 [Attribute ID] フィールドに、ここに示されるとおり「memberOf」と入力します。大文字と小文字の区別は重要です。

ステップ 4 [Value] フィールドで、ドロップダウン リストを使用して [=] を選択し、隣のフィールドに「Engineering」と入力します。

ステップ 5 [Attribute ID] フィールドに、ここに示されるとおり「memberOf」と入力します。大文字と小文字の区別は重要です。

ステップ 6 [Value] フィールドで、ドロップダウン リストを使用して [=] を選択し、隣のフィールドに「Employees」と入力します。

ステップ 7 AAA 属性タイプとしては、ドロップダウン リストを使用して [Cisco] を選択します。

ステップ 8 [Tunnel] グループ ボックスをオンにし、ドロップダウン リストを使用して [=] を選択し、隣のドロップダウン リストで適切なトンネル グループ（接続ポリシー）を選択します。

ステップ 9 [Access Policy Attributes] 領域の [Network ACL Filters] タブで、前のステップで定義した DAP 基準を満たすユーザーに適用する ACL を選択します。

DAP を使用してセッショントークンのセキュリティを確認する

ASA がセキュアクライアントからの VPN 接続要求を認証すると、ASA はセッショントークンをクライアントに返します。AnyConnect 4.9（MR1）以降、ASA とセキュアクライアントは、セッショントークンのセキュリティを強化するメカニズムをサポートします。セキュアクライアントがセッショントークンのセキュリティをサポートするように、DAP を設定する必要があります。

DAP をエンドポイント属性設定と一緒に使用し、LUA スクリプトを使用して、トークンセキュリティをサポートしていないセキュアクライアントバージョンからの接続試行を拒否します。

手順

ステップ 1 ASDM では、**[設定（Configuration）]** > **[リモートアクセス VPN（Remote Access VPN）]** > **[ネットワーク（クライアント）アクセス（Network (Client) Access）]** > **[ダイナミックアクセ**

スポリシー（Dynamic Access Policies）]>[ダイナミックポリシーの追加/編集（Add/Edit Dynamic Access Policy）]を選択します。

ステップ 2 エンドポイント属性の選択領域で、[追加（Add）] をクリックします。

a) [エンドポイント属性タイプ（Endpoint Attribute Type）] ドロップダウンで、[アプリケーション（Application）] を選択します。
b) [クライアントタイプ（Client Type）] で、等号 (=) 演算子を選択し、ドロップダウンからセキュアクライアントを選択します。
c) [OK] をクリックします。

ステップ 3 [Advanced（詳細設定）] の選択基準を設定します。

a) [AND] 演算子を選択します。
b) **論理式**の追加

```
(type(endpoint.anyconnect.session_token_security)~="string" or
EVAL(endpoint.anyconnect.session_token_security,"NE","true","string"))
```

ステップ 4 [アクション（Action）] 領域で、[終了（Terminate）] を選択します。

ステップ 5 オプションのユーザーメッセージを追加し、[OK] をクリックします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。